CLAIMS

1 – 23. (canceled)

24. (previously presented) A method of device authentication, the method comprising:

receiving, at a printer cartridge comprising a roaming device, a challenge from a host printer device;

generating, at the printer cartridge comprising the roaming device, a first nonreversible computation result, wherein the first nonreversible computation result is computed by seeding a first nonreversible algorithm with at least the challenge, and a roaming device secret;

outputting to the host printer device a response to the challenge, wherein the outputted response includes the first nonreversible computation result,

outputting to the host an identification and at least another data item;

generating, at the host printer device a second nonreversible computation result, wherein the second nonreversible computation result is computed by seeding a second nonreversible algorithm with at least a challenge and a host printer device secret;

comparing, by said host printer device, said first nonreversible computation and said second nonreversible computation in order to authenticate the printer cartridge comprising the roaming device;

allowing said host printer device to print documents if said printer cartridge comprising said roaming device is authenticated.

25. - 26. (canceled)

27. (previously presented) The method of claim 24, further comprising:

enabling said printer cartridge to operate responsive to a positive authentication of the roaming device.

28. (previously presented) The method of claim 24, further comprising:

disabling said host printer device responsive to a failure to authenticate the roaming device.

29. (previously presented) The method of claim 24, wherein the first nonreversible computation result is computed by further seeding the first nonreversible algorithm with a unique device identifier.

30. - 34. (canceled)

35. (currently amended) A host system device and subsystem device combination comprising:

a host security circuit, said host security circuit comprising:

at least one locally stored secret,

seed data;

a host processor for performing a non-reversible device authentication algorithm; and

means for reading data from a subsystem device;

a roaming security device as part of said subsystem device, said roaming security device comprising;

a subsystem processor for performing non-reversible computations;

a memory component, connected to said subsystem processor, said memory circuit comprising at least one secret;

a communication circuit, connected to said subsystem processor, for communicating with said host security circuit;

said subsystem device being removably attached to said host system device, said host system being ~~substantially~~ a printer and being inoperable for printing without being attached to said subsystem device.

36. (previously presented)The host system device and subsystem device combination of claim 35, wherein said host security circuit sends a challenge to said roaming security device and said roaming security device provides a first response to said challenge, using said at least one secret, to said host security circuit.

37. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 36, wherein said host security circuit reads said first response from said roaming security device and said host security circuit compares said first response with a first result of said non-reversible device authentication algorithm to determine if said first response and said first result match.

38. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said roaming security device authenticates said host security circuit ~~at substantially the same time as~~ while the host security circuit authenticates said roaming security device.

39. (canceled)

40. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said subsystem device is a printer cartridge.

41. (not entered)

42. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said host security circuit periodically checks the authenticity of said roaming security device.

43. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein communication data is encrypted prior to communication between said host system device and said subsystem device.

44. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein an attempt to physically access the circuitry of the roaming security device results in the destruction of data stored in said roaming security device.

45. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said subsystem device further comprises a battery for at least partially powering said roaming security device.

46. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said at least one locally stored secret is never communicated to said subsystem device.

47. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said at least one secret is never communicated to said host device.

48. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said non-reversible device authentication algorithm is a SHA-1 algorithm.

49. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said host security circuit communicates with said subsystem device to authenticate said subsystem device and to determine at least one of whether said subsystem device is the proper type, brand, or age.

50. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 49, wherein said host system is disabled if said subsystem device cannot be authenticated.

52. (currently amended) The host ~~security~~ system device and subsystem device combination of claim 35, wherein said subsystem device is a consumable device.

51. (currently amended) A subsystem device comprising:

a replaceable subsystem that operationally completes a host system, said host system being a printer device;

a security device being a part of said replaceable subsystem, said security device comprising:

a first memory portion configured to store a device ID;

a second memory portion configured to store at least one device secret;

a processor connected to said first and second memory portions, the processor configured to read the stored device ID from the first memory portion, the at least one stored device secret from the second memory portion and to perform a nonreversible computation using the device ID, the at least one device secret and a challenge as seeds; and

a communication circuit connected to the processor, said communication circuit configured to receive the challenge from a host device and to communicate a result of the nonreversible computation, performed by the processor, back to the host for authentication of said replaceable subsystem.

52. (previously presented)The subsystem device of claim 51, wherein said host device is disabled until a replaceable subsystem is installed and authenticated.

53. (canceled)

54. (previously presented)The subsystem device of claim 51, wherein said subsystem is a consumable device.

55. (previously presented)The subsystem of claim 51, wherein said subsystem is a printer cartridge.

56. (previously presented)The subsystem of claim 51, wherein said nonreversible computation is a SHA-1 computation.

57. (previously presented)The subsystem of claim 51, wherein said subsystem authenticates said host.

58. (previously presented)The subsystem of claim 51, wherein an attempt to physically access said security device will result in the destruction of said device ID and said at least one device secret.